UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/758,889	01/16/2004	Pratik M. Mehta	016295.1518 (DC-05677)	6993

23640 7590 07/14/2008

BAKER BOTTS, LLP
910 LOUISIANA
HOUSTON, TX 77002-4995

EXAMINER	
WANG, HARRIS C	

ART UNIT	PAPER NUMBER
2139	

NOTIFICATION DATE	DELIVERY MODE
07/14/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

debbie.allen@bakerbotts.com

Office Action Summary	Application No.	Applicant(s)	
	10/758,889	MEHTA ET AL.	
	Examiner	Art Unit	
	HARRIS C. WANG	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 March 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-10 and 21-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 4-10, 21-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

The Examiner finds the Applicants argument that the references Sun and Day do not teach, disclose or suggest a "wireless network...such that at least a first wireless client and a second wireless client can access the wireless network without authentication (Remarks pg. 9)" to be persuasive.

A new rejection follows.

Claim Rejections - 35 USC § 102

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 21-23, 25, 30 are rejected under 35 U.S.C. 102(b) as being anticipated by Yamaguchi (20020178365).

Regarding Claim 1, 21-23, 25, 30

Yamaguchi (20020178365) teaches a method for activating a wireless network security with a wireless host *("The encryption may be carried out according to the Wired Equivalent Privacy ("WEP") encryption standard commonly used in wireless networks, although any other type of encryption or security protection may be utilized" Paragraph [0024])* , comprising:

in a wireless network having a deactivated wireless network security for the wireless network such that at least a first wireless client and a second wireless client can access the wireless network without authentication, a wireless host establishing a communication connection with the first client *(Figure 2A. shows an intermediate device which allows 2 different modes for the wireless LAN card, "Driver for Wireless LAN Card (encrypted)* ***54,*** *and "Driver for Wireless LAN (no encryption)* ***56****) The Examiner interprets the wireless LAN card* ***56*** *of Figure 2A to be the "wireless network having a deactivated wireless network security" as in the claimed language. If there is no encryption, it is inherent that the two computing devices in Figure 1A (Computing Devices* ***2*** *and* ***6****) can access the unencrypted wireless network without authentication)* ;

in response to the communication connection, the wireless host automatically requesting from the first client a determination of whether to activate the wireless network security; *("When a user logs onto a computer network, directory services…may be utilized to control the administration of a computer network…to control what particular network resources a user has...the login server…may query the intermediate device to determine the security parameters (e.g. to determine whether encryption is on or off, or the level of encryption" Paragraph [0033])*

the wireless host receiving from the first client a determination to activate the wireless network security; in association with the determination to activate the wireless security network, the wireless host receiving an identifier code from the first client; the wireless host determining that the received identifier code from the first client matches a unique key-code maintained by the wireless host *("In order to use such WEP encryption, the user sets the same encryption key in both the end client or the laptop computer,*

and also the access point which communicates with the wireless device" Paragraph [0005]) The Examiner interprets the "received identifier code" as the encryption key used to set up WEP

and as a result of determining that the received identifier code from the first client matches the unique key-code maintained by the wireless host, the wireless host activating the deactivated wireless security network for the wireless network such that the second client cannot access the wireless network without authentication *("when the security level is set to a relatively high level, or encryption is on, for example, access to a file server which is one of the network resources may be permitted. Access to the file server may be denied unless encryption is on" Paragraph [0031])*.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was

not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 4-5, 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamaguchi in view of Sullivan (20030154287).

Regarding Claims 4-5, 26, 31

Yamaguchi teaches the method of Claim 1.

Yamaguchi does not teach further comprising following the activation of the wireless security network, changing the unique key-code to a personal code selected by the first client, further comprising resetting the unique key-code to a factory default.

Sullivan teaches the user changing the unique key-code to a personal code, and then resetting the unique key-code to a factory default *("If the customer is connected wirelessly to the access point and opens the access point's user interface and changes the settings, he is at that point in time cut off form the access point and the rest of the network. If he cannot subsequently make the same changes on his client (perhaps he forgot to write down the encryption key) he is out of luck, and must reset the access point. If the access point is in a router, the hardware reset will reset everything, including his WAN settings, so his Internet Access is lost" Paragraph [0003])*

.It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Yamaguchi to further include changing the password from default and then resetting to factory default.

The motivation to change the password from default is for an easier time memorizing the password, and the motivation to reset to default is if the client "forgets to write down the encryption key."

Claim 24 rejected under 35 U.S.C. 103(a) as being unpatentable over Yamaguchi in view of Wu (20030200455).

Regarding Claim 24,

Yamaguchi teaches the method of Claim 1. Yamaguchi does not explicitly teach wherein the unique key-code is a local area network (LAN) media access control (MAC) address supplied with the wireless host.

Wu (20030200455) teaches using a MAC address as a code. *("When a new wireless station is found having a correct SSID, a correct key value of the Wired Equivalent Privacy (WEP), and a pre-registered Media Access Control address (MAC address) on the Access Point, an association is to be made between the wireless station and the wireless base station (Paragraph [0051]))*

It would have been obvious to one of ordinary skill in the art at the time of the invention to use a pre-registered MAC address as a code.

The references above teach all the of the claimed limitations (unique key-code, MAC address, WEP). One of ordinary skill in the art could have combined the elements as claimed by known methods (using a number (MAC address) as a code), and the combination would have yielded predictable results to one of ordinary skill in the art at the time of the invention (the MAC address would be the code).

Claims 6-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yamaguchi in view of Serceki further in view of Windows ME.

Regarding Claims 6-9, 27-29, 32

Yamaguchi teaches the method of Claim 1, further comprising:
the wireless host receiving from the first client a determination not to activate the wireless network security *(Figure 2A. shows an intermediate device which allows 2 different modes for the wireless LAN card, "Driver for Wireless LAN Card (encrypted)* ***54,*** *and "Driver for Wireless LAN (no encryption).*

Yamaguchi does not explicitly teach and in response to the received determination not to activate the wireless network security, the wireless host setting a reminder flag such that the first client is automatically reminded at a future time to activate the wireless network security wherein the remainder flag comprises:

a reminder time period such that the first client is automatically reminded to activate the wireless security network after the expiration of the reminder time period.

a reminder condition such that the first client is automatically reminded to activate the wireless security network upon a subsequent communication connection.

a never-reminder response such that the first client is not subsequently reminded to activate the wireless network security.

Serceki (20030078072) requires the network administrator to regularly update the WEP keys at a regular intervals. *("The sequence 400 begins when a network administrator decides to change security (WEP) keys for the wireless network. Depending on internal policies, the network administrator may be required to change the security keys at regular intervals or after detecting a security breach" Paragraph [0032])*

The combined references still do not teach the wireless host setting a reminder flag such that the first client is automatically reminded at a future time to activate the wireless network security wherein the remainder flag comprises: a reminder time period such that the first client is automatically reminded to activate the wireless security network after the expiration of the reminder time period.

a reminder condition such that the first client is automatically reminded to activate the wireless security network upon a subsequent communication connection.

a never-reminder response such that the first client is not subsequently reminded

Windows Millennium Edition (released in 2000) teaches

If no connection exists, Automatic Updates are suspended until the next connection occurs before checking for or downloading updates.

Automatic Updates are designed to check for updates every 24 hours. If there are no updates available, Automatic Updates resets and then checks again in 24 hours after the Internet connection is established. If the download is interrupted, Automatic Updates resumes at a later time when there is available bandwidth.

You can configure Automatic Updates by using the Automatic Updates tool in Control Panel. There are three settings:

- Automatically download updates and notify me when they are ready to be installed.
- Notify me before downloading any updates and notify me again when they are ready to be installed.
- Turn off Automatic updating. I will update my computer manually.

The default setting is "Automatically download updates and notify me when they are ready to be installed".

The Examiner interprets "a never reminder" in the claimed language as updating manually. The Examiner interprets "automatically updating in a time period" as checking for updates eveyr 24 hours. The Examiner interprets activating "upon a subsequent connection" as automatic updates are suspended until the next connection.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of Yamaguchi, which teaches the option of enabling or disabling network security, and the method of Serceki, which teaches updating the network security keys on a regular interval with the updating methods taught by Windows ME.

The above references teach all the claimed elements (enabling and disabling network security, changing the security keys at regular intervals) and one skilled in the art could have combined the elements as claimed by known elements (updating according to Windows Automatic Updates as taught in Windows ME) and the

combination would have yielded predictable results to one of ordinary skill in the art at the time of the invention (a reminder to update the network security comprising: reminding upon the next connection, reminding automatically, reminding after a given time period, or never reminding)

Regarding Claim 10,

Yamaguchi, Serceki and Windows ME teach the method of Claim 6. Yamaguchi teaches further comprising registering the first client to save configuration information on the client such that the wireless host recognizes the first client on a subsequent communication connection. *(Figure 4 shows setting communication and security parameters)*

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HARRIS C. WANG whose telephone number is (571)270-1462. The examiner can normally be reached on M-F 9-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, KRISTINE KINCAID can be reached on (571) 272-4063. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

HCW

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139